

MENU

SEARCH

INDEX

DETAIL

1/1



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11)Publication number: 11039219

(43)Date of publication of application: 12.02.1999

(51)Int.Cl.

G06F 12/14  
 G06F 9/06  
 G09C 1/00  
 G09C 1/00  
 H04L 9/32

(21)Application number: 09193535

(22)Date of filing: 18.07.1997

(71)Applicant:

(72)Inventor:

FUJI XEROX CO LTD

KONO KENJI

TAGUCHI MASAHIRO

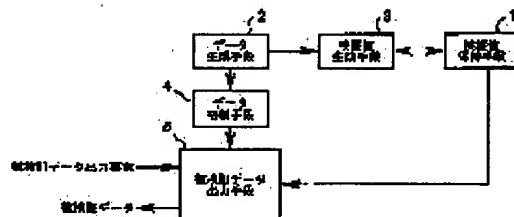
SAITO KAZUO

(54) DATA-TO-BE-VERIFIED GENERATING DEVICE, DATA VERIFYING DEVICE, AND MEDIUM RECORDING  
 VERIFIED DATA GENERATING PROGRAM

(57)Abstract:

**PROBLEM TO BE SOLVED:** To generate data which can be kept in a terminal device in such a state that the data is not used in an unauthorized state and for which the compatibility of order is guaranteed.

**SOLUTION:** A verified value holding means 1 holds a verified value and a data generating means 2 generates a data main body at prescribed timing. A verified value generating means 3 generates a new verified value based on the verified value held by the holding means 1 and a newly generated data main body whenever the data generating means 2 generates a data body and updates the verified value held by the holding means 1 with the new verified value. A data storing means 4 successively stores the data bodies generated by means of the data generating means 2. A data-to-be-verified outputting means 5 generates an authenticator based on the verified value held by the holding means 1 and outputs data to be verified which are generated by coupling the generated authenticator with the data main body stored in the data storing means 4 upon receiving a data-to-be-verified outputting request.



LEGAL STATUS

[Date of request for examination]  
[Date of sending the examiner's decision of rejection]  
[Kind of final disposal of application other than the  
examiner's decision of rejection or application converted  
registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision of  
rejection]  
[Date of requesting appeal against examiner's decision of  
rejection]  
[Date of extinction of right]

---

Copyright (C); 1998 Japanese Patent Office

---

[MENU](#)[SEARCH](#)[INDEX](#)[DETAIL](#)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-39219

(43) 公開日 平成11年(1999) 2月12日

(51) Int.Cl. <sup>8</sup>	識別記号	F I
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14 3 1 0 Z
9/06	5 5 0	9/06 5 5 0 Z
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00 6 4 0 A
	6 6 0	6 6 0 A
H 0 4 L 9/32		H 0 4 L 9/00 6 7 3 E
審査請求 未請求 請求項の数9 O L (全 15 頁)		

(21) 出願番号 特願平9-193535

(22) 出願日 平成9年(1997) 7月18日

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 河野 健二

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

(72) 発明者 田口 正弘

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

(72) 発明者 齊藤 和雄

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

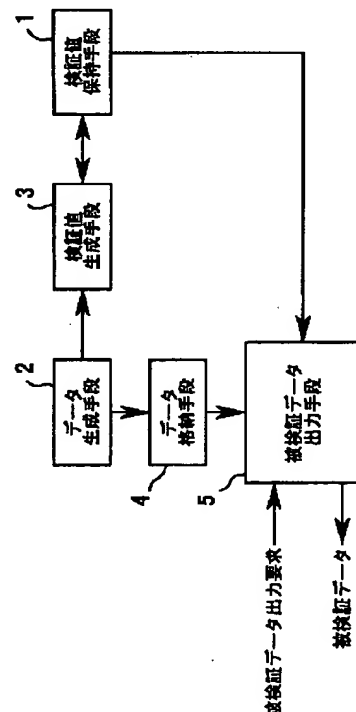
(74) 代理人 弁理士 服部 毅巖

(54) 【発明の名称】 被検証データ生成装置、データ検証装置及び被検証データ生成プログラムを記録した媒体

(57) 【要約】

【課題】 不正操作を受けることなく端末装置に保管可能であり、且つ順番の整合性が保証されたデータを生成できるようにする。

【解決手段】 検証値保持手段1は、検証値を保持する。データ生成手段2は、所定のタイミングでデータ本体を生成する。検証値生成手段3は、データ生成手段2によりデータ本体が生成される度に、検証値保持手段1において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成する。そして、新たな検証値で検証値保持手段1に保持されている検証値を更新する。データ格納手段4は、データ生成手段2で生成されたデータ本体を順次格納する。被検証データ出力手段5は、被検証データ出力要求を受け取ると、検証値保持手段1に格納されている検証値に基づいて認証子を生成し、生成した認証子とデータ格納手段4に格納されているデータ本体とを結合した被検証データを出力する。



## 【特許請求の範囲】

【請求項1】 被検証データを生成する被検証データ生成装置において、  
検証値を保持する検証値保持手段と、  
データ本体を生成するデータ生成手段と、  
前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段と、  
前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段と、  
被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力手段と、  
を有することを特徴とする被検証データ生成装置。

【請求項2】 データ消去要求に応じて、前記データ格納手段に格納されているデータ本体を消去するデータ消去手段と、  
前記データ消去手段によって前記データ格納手段内のデータが消去される度に設定されている値をカウントする被検証データシリアル番号カウンタとをさらに有し、  
前記被検証データ出力手段は、被検証データ出力要求を受け取った際の前記被検証データシリアル番号カウンタの値を前記被検証データに含めて出力することを特徴とする請求項1記載の被検証データ生成装置。

【請求項3】 前記検証値生成手段は、一方向性関数を用いて新たな検証値を生成することを特徴とする請求項1記載の被検証データ生成装置。

【請求項4】 前記データ生成手段によるデータ本体の生成条件を保持するデータ生成条件保持手段と、  
前記データ生成条件が満たされなくなった時点で、所定のデータ処理機能を停止する機能停止手段と、  
利用延長データを受け取ると、前記利用延長データを認証する利用延長データ認証手段と、  
前記利用延長データ認証手段が認証に成功した場合に、前記データ処理機能の機能停止を解除する機能停止解除手段と、  
をさらに有することを特徴とする請求項1記載の被検証データ生成装置。

【請求項5】 前記利用延長データ認証手段は、受け取った利用延長データから照合用検証値を抽出し、前記照合用検証値と前記検証値保持手段に保持されている検証値とが一致した場合に限り前記利用延長データを認証することを特徴とする請求項4記載の被検証データ生成装置。

【請求項6】 前記利用延長データ認証手段は、受け取った前記利用延長データから照合用検証値を抽出すると

ともに、前記データ格納手段内のデータ本文を格納された順に選択し、最初に選択されたデータ本文と前記照合用検証値とから前記検証値生成手段と同じ方法で新たな検証値を生成し、以後、選択されたデータ本文と直前に生成された検証値とから新たな検証値を順次生成し、最後に生成された検証値と前記検証値保持手段に保持されている検証値とが一致した場合に限り前記利用延長データを認証することを特徴とする請求項4記載の被検証データ生成装置。

【請求項7】 前記被検証データ出力手段が被検証データを出力した時点で前記検証値保持手段に保持されている検証値をデータ出力時検証値として保持するデータ出力時検証値保持手段を更に有し、  
前記利用延長データ認証手段は、受け取った前記利用延長データから照合用検証値を抽出し、前記照合用検証値と前記データ出力時検証値保持手段に保持されているデータ出力時検証値とが一致している場合に限り前記利用延長データを認証することを特徴とする請求項4記載の被検証データ生成装置。

【請求項8】 データの検証を行うデータ検証装置において、  
検証値を保持する検証値保持手段と、  
複数のデータ本文に対して署名値が付加された被検証データを受け取ると、前記検証値保持手段に保持されている検証値と前記複数のデータ本文とから照合用検証値を生成する照合用検証値生成手段と、  
前記署名値から求められる検証値と前記照合用検証値とを照合し、一致した場合にのみ前記被検証データの内容が正しいと認める認証手段と、  
前記署名値から求められる検証値と前記照合用検証値とが一致した場合には、前記照合用検証値によって前記検証値保持手段に保持されている検証値を更新する検証値更新手段と、  
を有することを特徴とするデータ検証装置。

【請求項9】 被検証データの生成をコンピュータに行わせるための被検証データ生成プログラムを記録した媒体において、  
検証値を保持する検証値保持手段、  
データ本体を生成するデータ生成手段、  
前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段、  
前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段、  
被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力

手段、

としてコンピュータを機能させるための被検証データ生成プログラムを記録した媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は被検証データ生成装置、データ検証装置及び被検証データ生成プログラムを記録した媒体に関し、特にデータ群に署名を施して被検証データを生成する被検証データ生成装置、署名が施された被検証データを検証するデータ検証装置及びデータ群に署名を施すための被検証データ生成プログラムを記録した媒体に関する。

【0002】

【従来の技術】 近年のネットワークの発達によって、さまざまな情報がデジタル化されネットワークを通じて流通する時代が到来している。デジタル化される情報としては、文字情報をはじめ静止画、動画、音声、プログラムなどがあり、我々はネットワーク上でこれらを組み合わせたさまざまなサービスを受けることが可能である。しかし、これらデジタル情報の大きな特徴であるコピーの容易性が、これまでネットワークでのデジタル情報の流通を阻害する要因となっていた。これは、デジタル情報をコピーするとオリジナルとまったく同じ物を生成することができるため、一旦流通したものが著作権者の意図しないところで無断で使用され、著作権者が得るべき正当な対価を回収し難いという問題に起因する。

【0003】 この問題を解決するため、最近ではCD-Showcase（米International Business Machine社の登録商標）のように、デジタル情報を暗号化して自由に流通させ、利用するには代金を支払って電話回線等で復号鍵を受け取り、デジタル情報を利用するようなシステムも登場している。ただし、この方法では、利用頻度に応じて課金することが出来ない。

【0004】 利用頻度に応じて課金するには、利用履歴等の課金情報を回収する必要がある。そして、利用履歴を回収するに当たっては、利用履歴もまたデジタル情報であるためその正当性を保証する仕組みが必要となる。

【0005】 そこで、特開平3-25605号公報の「課金情報送出方式」および特開平6-180762号公報の「課金情報収集システム」に開示されているように、課金情報を出力する装置を通信回線で結んで自動的に課金情報を回収することが考えられている。なお、通信回線を利用する場合は、RSA (Rivest, Shamir, Adleman) 暗号を利用した電子署名方式（岡本栄司著：暗号理論入門、共立出版、pp. 134-138（1993））等により、課金情報の正当性を保証できる。

【0006】 なお、上記の例は、デジタル情報を利用する端末が常にネットワークにつながっていることが前提となっている。それは、オフラインの端末装置に履歴

データを長期にわたって蓄積すると、ユーザの恣意的な管理や、システムの事故などの危険にさらされるという弊害があるためである。ところが、一般的なユーザはデジタル情報をオフラインで利用することがほとんどである。そのため、ユーザの端末を常にネットワークで管理することは通信コストやシステムの運用性を考えると受け入れ難いものであるといえる。

【0007】 一方、秘密情報を保持する媒体としてIC (Integrated Circuit) カードが注目を集めている。このICカードを用いれば、課金情報等を安全に回収することができる。ICカードを用いて課金情報を回収するものとして、例えば、特公平6-95302号公報の「ソフトウェア管理方式」がある。これには、ソフトウェアを利用した量に応じて課金し、料金を回収するシステムの例が示されている。この例によれば、ユーザは所定の代理店でICカードを購入し、購入した代金に応じた金額がICカードの残高メモリに書き込まれる。ユーザがソフトウェアを起動する際にICカード内の残高メモリをチェックし、そのソフトウェアの利用価格分の金額を残高メモリから減算する。ユーザは、そのICカードの利用可能金額だけ利用すると、ICカードをSS協会（ソフトウェアを管理する協会）に届ける。ICカードにはユーザが利用したソフトウェアの利用明細が格納されており、SS協会はこの利用明細をもとにソフトウェアの著作権者に利用料金を支払う。これにより、ソフトウェアのオフラインでの使用を認めながらも、利用頻度に応じた課金が可能となる。

【0008】

【発明が解決しようとする課題】 しかし、利用明細を格納したICカードをSS協会に送付する方法では、ICカードの利用可能金額がなくなる度に、SS協会から再配布されるのを待つか、代理店で新しいICカードを購入しなければならないという問題点がある。しかも、一般的に履歴データは長大なものになる傾向があるため、ICカードのような記憶容量の少ない媒体に保管すると、頻繁にICカードを交換する必要性が出てくる。

【0009】 そのため、ICカードが生成する課金情報のように確実にセンタに送られるべきデータを、端末装置等に安全に保管できるような技術が必要とされている。すなわち、端末装置に課金情報を保管しておくことができれば、ICカードの記憶容量が少なくても、頻繁にICカードの再発行などをする必要がなく、しかも、オフラインでサービスを利用することができる。さらに、課金情報などの履歴データは数回または数十回に渡って出力されると考えられるため、履歴データの順番の整合性（連鎖）が保たれている必要がある。そして、センタでは、連鎖が崩されていないことを含めて検証できなければならない。なぜなら、途中の履歴データが抜けられていることを検出できないと、その部分の利用料金を回収できなくなるからである。

【0010】本発明はこのような点に鑑みなされたものであり、不正操作を受けることなく端末装置に保管可能であり、且つ順番の整合性が保証されたデータを生成できる被検証データ生成装置を提供することを目的とする。

【0011】また、本発明の他の目的は、不正操作を受けることなく端末装置に保管可能な形式のデータの連鎖性を含めて検証できるデータ検証装置を提供することである。

【0012】また、本発明の別の目的は、不正操作を受けることなく端末装置に保管可能であり、且つ順番の整合性が保証されたデータをコンピュータに生成させるための被検証データ生成プログラムを記録した媒体を提供することである。

【0013】

【課題を解決するための手段】本発明では上記課題を解決するために、被検証データを生成する被検証データ生成装置において、検証値を保持する検証値保持手段と、データ本体を生成するデータ生成手段と、前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段と、前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段と、被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力手段と、を有することを特徴とする被検証データ生成装置が提供される。

【0014】この被検証データ生成装置によれば、データ生成手段がデータ本体を生成すると、検証値生成手段により、検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値が生成され、生成した検証値で検証値保持手段に保持されている検証値が更新される。一方、データ生成手段で生成されたデータ本体は、順次データ格納手段に格納される。そして、被検証データ出力要求を受け取ると、被検証データ生成装置により、検証値保持手段に格納されている検証値を用いて署名値が生成され、データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データが出力される。

【0015】また、上記課題を解決するために、データの検証を行うデータ検証装置において、検証値を保持する検証値保持手段と、複数のデータ本文に対して署名値が付加された被検証データを受け取ると、前記検証値保持手段に保持されている検証値と前記複数のデータ本文とから照合用検証値を生成する照合用検証値生成手段と、前記署名値から求められる検証値と前記照合用検証

値とを照合し、一致した場合にのみ前記被検証データの内容が正しいと認める認証手段と、前記署名値から求められる検証値と前記照合用検証値とが一致した場合には、前記照合用検証値によって前記検証値保持手段に保持されている検証値を更新する検証値更新手段と、を有することを特徴とするデータ検証装置が提供される。

【0016】このデータ検証装置によれば、複数のデータ本文に対して署名値が付加された被検証データを受け取ると、照合用検証値生成手段により、検証値保持手段に保持されている検証値と複数のデータ本文とから照合用検証値が生成される。そして、認証手段により、署名値から求められる検証値と照合用検証値とが照合され、一致した場合にのみ被検証データの内容が正しいと認められる。一方、署名値から求められる検証値と照合用検証値とが一致した場合には、検証値更新手段により、検証値保持手段に保持されている検証値が、照合用検証値に更新される。

【0017】また、上記課題を解説するために、被検証データの生成をコンピュータに行わせるための被検証データ生成プログラムを記録した媒体において、検証値を保持する検証値保持手段、データ本体を生成するデータ生成手段、前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段、前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段、被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力手段、としてコンピュータを機能させるための被検証データ生成プログラムを記録した媒体が提供される。

【0018】この媒体に記録されたプログラムをコンピュータに実行させれば、検証値を保持する検証値保持手段と、データ本体を生成するデータ生成手段と、前記データ生成手段によりデータ本体が生成される度に、前記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成し、生成した検証値で前記検証値保持手段に保持されている検証値を更新する検証値生成手段と、前記データ生成手段で生成されたデータ本体を順次格納するデータ格納手段と、被検証データ出力要求を受け取ると、前記検証値保持手段に格納されている検証値を用いて署名値を生成し、前記データ格納手段に格納されているデータ本体と前記署名値とを含む被検証データを出力する被検証データ出力手段と、の各処理機能を持ったコンピュータシステムが構築される。

【0019】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は、本発明の原理構成図である。本発明の被検証データ生成装置は、以下のような要素で構成される。

【0020】検証値保持手段1は、検証値を保持する。データ生成手段2は、所定のタイミングでデータ本体を生成する。例えば、所定のデータ処理要求を受け取った際に、そのデータ処理の履歴をデータ本体として生成する。

【0021】検証値生成手段3は、データ生成手段2によりデータ本体が生成される度に、検証値保持手段1において保持されている検証値と新たに生成されたデータ本体とに基づいて新たな検証値を生成する。そして、新たな検証値で検証値保持手段1に保持されている検証値を更新する。データ格納手段4は、データ生成手段2で生成されたデータ本体を順次格納する。被検証データ出力手段5は、被検証データ出力要求を受け取ると、検証値保持手段1に格納されている検証値に基づいて認証子を生成し、生成した認証子とデータ格納手段4に格納されているデータ本体とを結合した被検証データを出力する。

【0022】これにより、データ処理要求が実行されるたびに、新たなデータ本体がデータ格納手段4に格納されるとともに、検証値保持手段1に保持されている検証値の内容が更新される。そして、被検証データ出力要求が出されると、検証値保持手段1内の検証値に基づく署名値で署名された被検証データが出力される。

【0023】このようにして出力された被検証データは、署名値が付加されているため、端末装置等に蓄えておいてもデータ本体の内容を改ざんすることができない。しかも、順次生成されるデータ本体とそれ以前に生成された検証値を用いて新たな検証値を生成するため、被検証データの連鎖性も保証される。すなわち、被検証データが多数生成された場合であっても、途中の被検証データが抜けた状態では、サーバなどの検証装置においてそのデータは認証されない。この結果、こまめに被検証データを外部に出力し、オフラインの端末装置などに保存しておくことができるようになり、データ格納手段4の記憶容量が少なくてすむ。

【0024】ところで、本発明の被検証データ生成装置は、ICカード上で実現することができる。この場合、履歴データをICカードに保持して媒体ごと送付するのではなく、ICカードに検証値を保持することで履歴データをICカードから取り出し、取り出した履歴データは一時的に端末装置に保存する。そして、ネットワークを用いて端末装置から履歴管理センタに履歴データを送付する。これにより、履歴データの正当性を保証しつつ、オフラインでの履歴の回収が可能となる。なお、電子署名等の技術を用いて履歴データ等を安全に取り出せるICカードは既に製品化されており、ISO(Interna-

tional Organization for Standardization)/IEC(International Electrotechnical Commission)-7816でもセキュアメッセージング技術として規定されている。

【0025】そこで、ICカードから履歴データなどの情報を端末装置へ取り出し、端末装置から任意のタイミングでセンタへ課金情報を転送する場合を例にとり、本発明の第1の実施の形態を以下に説明する。

【0026】図2は、ICカードを用いた履歴管理システムの概略構成を示す図である。ユーザが使用するパーソナルコンピュータ(PC)110は、インターネットなどのネットワーク120を介して履歴管理センタ130と繋がっている。履歴管理センタ130では、ユーザの登録および、ユーザデータやユーザに提供したサービスの履歴等の管理が行われる。そして、履歴管理センタ130は、PC110からの要求に応じて、カプセル化されたソフトウェア(以下、単に「カプセル」という)300を提供する。ここでいうカプセル化とは、例えばDES(Data Encryption Standard)等の暗号アルゴリズムを用いて暗号化し、そのままでは使用できないようにすることを指す。なお、カプセル300は、CD-ROM等の媒体でユーザに提供することもできる。

【0027】また、PC110には、RS-232C(アメリカ電子工業会によって規定されたデータ通信用インタフェース)などのインタフェースにより、リーダ/ライタ140が接続されている。ユーザは、このリーダ/ライタ140にICカード200を接続することで、履歴管理センタ130から取得したソフトウェアの復号鍵や使用履歴を取得できる。

【0028】ICカード200は、ソフトウェアを提供するプロバイダ若しくはプロバイダの依頼を受けた履歴管理センタ130からユーザに渡されるものである。なお、この例では、PC110によってサービスを利用するものとしているが、サービスを利用するためのローカルな端末装置はPCには限定されず、例えばワークステーションであったり、サーバであったり、ATM(Auto Teller Machine)端末であったりする。

【0029】図3は、カプセル化されたソフトウェアの構成を示す図である。カプセル300の内容は、ヘッダ部310と、暗号化されたソフトウェア320とに分かれている。ヘッダ部310には、カプセルを識別するためのカプセルID311、利用料金を算出するための課金情報312、及びソフトウェアの復号鍵を生成するための復号鍵生成データ313が含まれている。なお、プロバイダにより作成されたソフトウェアは、センタまたはそれに準ずる機関によりカプセル化される。

【0030】図4は、ICカードのハードウェア構成を示す図である。ICカード200は、CPU210を中心として、1つのコンピュータシステムが構築されている。CPU210には、内部のシステムバスを介して他

の各種要素が接続されている。RAM(Random Access Memory) 220は、CPU210が処理すべきデータを一時的に格納する。ROM(Read Only Memory) 230は、ICカード200に必要な機能をCPU210に実行させるためのプログラムが格納されている。入出力装置(I/O) 240は、所定の規格に従って、リーダ/ライタ140との間でデータ通信を行う。PROM(Programmable Read Only Memory) 250は、暗号化された復号鍵生成データ313から復号鍵を生成するための秘密情報などが格納されている。なお、上記のPROM250は、データの書き換えが可能であり、且つ電源の供給が無くてもデータを保持できる記憶装置(不揮発性メモリ)であれば、他の記憶装置であってもよい。

【0031】このようなハードウェア構成のICカード200によって、以下のような処理機能を実現されている。図5は、ICカードの処理機能を示すブロック図である。

【0032】ログ生成部201は、PC110からヘッダ部を受け取ると、ログを生成する。ただし、ログ数カウンタ204aの値が格納可能ログ数201aの値と等しい場合には、ログを生成せずにPC110に対してエラーを返す。格納可能ログ数201aは、ログセット格納部204に格納できるログの数が予め設定されており、その値はICカード200のPROM250の容量によって定まる。

【0033】検証値格納部202には、ログの連鎖が正しいことをICカード110と履歴管理センタ130とで検証するための検証値が格納されている。検証方法については後述する。

【0034】MD5演算部203は、ログ生成部201で新たなログが生成される度に、新たな検証値を生成する。具体的には、まず、ログ生成部201で生成されたログと検証値格納部202に格納されている検証値とを結合する。さらに、結合された値に対して一方向性ハッシュ関数「MD5」(R.Rivest:The MD5 Message-Digest Algorithm, Internet RFC 1321(1992))を用いてメッセージ・ダイジェストを計算し、検証値を生成する。そして、生成された検証値を用いて、検証値格納部202内の検証値の値を更新する。

【0035】なお、上記の例では一方向性ハッシュ関数「MD5」を用いて検証値を生成しているが、ここでいう一方向性とは計算結果から計算される前の値を逆算することができないことを指し、このような性質を持つか、あるいは持つと思われる関数であれば「MD5」と代替可能である。

【0036】ログセット格納部204は、複数のログの組であるログセットを格納しており、ログ生成部201が生成したログを逐次ログセットに連結する。ログ数カウンタ204aは、ログセット格納部204に格納されたログ数をカウントしている。このカウンタの値は、ロ

グセット格納部204内のログセットが消去された際に「0」にリセットされる。

【0037】復号鍵生成部205は、ログ生成部201でログが生成されると、ICカード200内の秘密データとカプセル300の復号鍵生成データ313とにより復号鍵を生成し、復号鍵をPC110に転送する。

【0038】ログ管理部206は、PC110からログセット出力要求を受け取ると、ログセット格納部204に格納されているログセットをPC110に対して出力する。なお、出力するログセットには、ログセットシリアル番号カウンタ206aの値を付加する。ログセットシリアル番号カウンタ206aは、ログセットの通し番号を格納しており、ログセットが消去される度に、値を1だけインクリメントする。また、ログセットの出力が可能であるか否かは、ログ出力状態206bによって管理している。ログ出力状態206bには、「FALSE」と「TRUE」とがある。「FALSE」の場合には、ログセットを出力することができず、「TRUE」の場合には、ログセットの出力が可能である。

【0039】稼働制御部207は、ログ生成部201の機能を含めICカード200の基本的な機能の起動と停止とを管理している。具体的には、利用期限207aの範囲を超えている場合、あるいは生成可能ログ数減算カウンタ207bの値が0である場合には、ICカード200の機能を停止する。そして、利用延長データ認証部208からの指令によって、停止していた機能を起動する。なお、利用期限207aは、ICカード200の利用期限が設定されている。生成可能ログ数減算カウンタ207bは、ログセットを履歴管理センタ130に送付せずにカプセルを利用可能な限度回数が初期値として設定されており、ログ生成部201によってログが生成される度に値が1だけ減算される。

【0040】利用延長データ認証部208は、PC110から利用延長データを受け取ると、利用延長データの認証を行う。そして、認証に成功した場合には、利用延長データを用いて、利用期限207aと生成可能ログ数減算カウンタ207bとを更新する。

【0041】以上のような機能を有するICカード200を用いて、カプセル300内の暗号化されたソフトウェア320を実行するには、次のような作業を行う。まず、ユーザは、ICカード200をリーダ/ライタ140に接続する。そして、PC110によってカプセル300に起動をかける。

【0042】図6は、カプセル実行開始手順を示すフローチャートである。この図において、点線の左側に示す処理はPC110で行われる処理であり、点線の右側に示す処理はICカードで行われる処理である。

【S1】PC110が、カプセル300内のヘッダ部310をICカード200へ転送する。

【S2】ヘッダ部310を受け取ったICカード200



では、まず、ログ生成部201が新たなログを生成し、そのログをMD5演算部203とログセット格納部204に渡す。

〔S3〕MD5演算部203が、受け取ったログと検証値格納部202に格納されている検証値とから新たな検証値を生成し、検証値格納部202内の検証値を更新する。

〔S4〕ログセット格納部204が、格納しているログセットに、受け取ったログを連結する。なお、この時、ログ出力状態206bが「TRUE」の場合には、ログ管理部206がログ出力状態206bを「FALSE」にする。

〔S5〕ログ数カウンタ204aが、保持している値を1だけカウントアップする。また、生成可能ログ数減算カウンタ207bが、保持している値を1だけカウントダウンする。

〔S6〕復号鍵生成部205が復号鍵生成データ313と秘密データとを用いて復号鍵を生成し、PC110へ転送する。

〔S7〕復号鍵を受け取ったPC110が、その復号鍵で暗号化されたソフトウェア320を復号し、実行する。

〔0043〕このようにして、ユーザがカプセル内のソフトウェアを実行する度に、その利用履歴がログとしてICカード200内で保持される。図7は、ログの構成例を示す図である。ログ400には、カプセルID401、ログ作成時刻402、及び課金情報403が含まれている。ところで、ログ400は一時的にICカード200内に格納されるので、各要素はできるだけ少ないバイト数で構成することが望ましい。たとえばシステム時刻をUTC(Coordinated Universal Time:世界協定時刻)に対応する4バイトで表現しているとする、ログ作成時刻にはUTC4バイトをすべて入れる必要はなく、たとえば細かい値が必要無いならば全4バイトのうち上位3バイトを入れればよく、また相対値のみがわかればよいなら下位3バイトを入れればよい。

〔0044〕次に、ICカード200の内部で保持されているログセットを履歴管理センタ130で回収し、その値を検証する方法について説明する。ログセット格納部204内の複数のログは、生成された順番に結合され、ログセットとしてICカード200内の不揮発性メモリ(PROM250)に格納されるが、ICカード200の記憶容量の関係から大量のログデータをICカード200内に記憶することは不可能であり、ICカード200には予め格納可能ログ数201aが設定されている。そして、ログ数カウンタ204aの値がこの格納可能ログ数201aに達すると、ログ生成部201が新たなログを生成できず、復号鍵生成部205も復号鍵を出力しない。したがって、このままではソフトウェアの実行ができない。

〔0045〕この状態になるとユーザはPC110を操作し、PC110からICカード200に対しログ出力要求を出す。ログ出力要求を受け取ったICカード200は、ログセットにICカード200の署名を施した署名付きログセットを出力する。ちなみにユーザはログ数一杯になる前にもログ出力を行うことが可能である。

〔0046〕図8は、署名付きログセットの構成を示す図である。署名付きログセット500は、ユーザID501、ログセット作成時刻502、ログセットシリアル番号503、署名値504、ログ数511およびn個のログ512とから構成される。

〔0047〕図9は、ログセットの署名値504として署名される平文の構成例を示す図である。ここではICカード200の署名鍵(秘密鍵)で署名される平文700を暗号化する場合について説明する。署名に用いる暗号化方式は公開鍵暗号方式に限らず履歴管理センタ130とICカード200で秘密鍵を安全な方法で共有できれば慣用鍵暗号方式を用いてもよい。

〔0048〕署名される平文700は、ユーザID701、ログセット作成時刻702、ログセットシリアル番号703、ログ数704および検証値705で構成される。検証値705はログセット500を出力するときにICカード200の検証値格納部202に保持されている検証値と同一のものである。すなわち、これらの情報からなる平文700をICカード200の秘密鍵で暗号化することで、署名値504が得られる。

〔0049〕図10は、ICカードからログセットを出力する手順を示すフローチャートである。この図において、点線の左側に示す処理はPC110で行われる処理であり、点線の右側に示す処理はICカードで行われる処理である。

〔S11〕PC110が、ICカード200に対してログセット出力要求を出す。

〔S12〕ICカード200では、ログ管理部206が、ログセット出力要求を受け取り、ログ出力状態206bを「TRUE」にし図8に示したような署名付きログセット500を出力する。

〔S13〕PC110が、ICカード200からログセットを取得する。

〔S14〕PC110は、ログセットを正常に取得できたか否かを判断する。ログセットをPC110が正常に取得できていればステップS15に進む。一方、ログセットが正常に取得できなかった場合は、ステップS11に進み、再度ICカード200に対してログセット出力要求を出し、ステップS11～S13を繰り返す。

〔S15〕PC110が、ICカード200に対してログセット消去要求を出す。

〔S16〕ICカード200では、ログ管理部206がログセット消去要求を受け取り、ログ出力状態206bが「TRUE」であるか否かを判断する。「TRUE」

であればステップS17に進み、「TRUE」でなければステップS21に進む。

〔S17〕ログ管理部206が、ログセット格納部204内のログセットを消去する。

〔S18〕ログ数カウンタ204aが、保持している値を「0」にリセットする。

〔S19〕ログセットシリアル番号カウンタ206aが、保持しているログセットシリアル番号を1だけインクリメントする。

〔S20〕ログ管理部206は、正常終了を表すステータスをPC110に返し、処理を終了する。

〔S21〕ログ出力状態206bが「FALSE」ならばログセットの消去は行わずエラーステータスをPC110に返す。

〔0050〕なお、ログセット出力中にエラーが発生した場合のことを考慮して、ICカード200をリセット状態にした場合はログ出力状態206bは「FALSE」となる。

〔0051〕以上がログセットを出力する手順であるが、このようにログセットの出力とログセットの消去を別々の命令で行うのは、以下のようなICカード200のプロトコル形式に依存した理由による。ICカード200のデータ転送プロトコルT=0およびT=1（ISO/IEC7816-3）では、ICカード200からIFD（Interface Device）（ここではPC110を示す）にデータを出力した後、ICカード200は受信待ち状態となりICカード内で処理を行うことができない。もし、1つのコマンドでログセットの出力と消去を行おうとすると、ログセットを消去した後でログセットを出力しなければならなくなるので、ログセットの出力が通信の過程で失敗した場合にログセットが失われてしまうことになる。

〔0052〕一方、単純にログセット出力コマンドとログセット消去コマンドの2つに分けただけだと、ユーザが誤ってログセットを出力する前にログセット消去コマンドをICカードに発行してしまうと、ログセットが失われてしまう。したがって本発明ではICカードにログ出力状態206bを持たせ、ログセット203が出力された場合のみログ出力状態206bが「TRUE」となりログセットが消去可能となることで、上記の問題を解決している。ログセット消去後、ソフトウェアの起動を行うと、ログがICカード内で生成され、ログ出力状態206bが「FALSE」状態となるので、再びログセット出力を行わない限りログセットを消去できない。

〔0053〕ICカード200から出力されたログセット500は、一旦PC110で保管される。PC110で保管されたログセット500はある一定期間ごとに履歴管理センタ130で回収して、そのログの内容を基にユーザから料金を徴収しソフトウェアの著作者に料金を分配する。履歴管理センタ130で効率よく履歴を回収

するために、ICカード200には利用期限207aと生成可能ログ数という2つの値があらかじめ設定されている。利用期限207aとはICカード200を利用可能な期日を表し、利用期限207aを過ぎた後はICカード200が停止状態となり、カプセルを利用できなくなる。再び利用可能とするためには履歴管理センタ130にこれまで出力したログセットを送信し利用延長データを取得する必要がある。また、生成可能ログ数は、生成可能ログ数減算カウンタ207bの初期値として設定され、生成可能ログ数減算カウンタ207bの値が0になるとICカード200が停止状態となり、カプセル300を利用できなくなる。再び利用可能とするためには、履歴管理センタ130にログセットを送信し利用延長データを取得する必要がある。

〔0054〕ところで、ユーザごとのログセットの検証を履歴管理センタで行うには、履歴管理センタ130において、以下のようなユーザデータベース（DB）を有している必要がある。

〔0055〕図11は、履歴管理センタで管理しているユーザDBの例を示す図である。ユーザDB900には、各ユーザの履歴管理用データ910がある。この履歴管理用データ910には、ユーザID911、前回検証したログセットの最終シリアル番号912、最終シリアル番号に対応するログセットの検証値913、及びその他認証等に用いるユーザ固有のデータ914が含まれている。

〔0056〕ユーザは上記の利用限度が来てカプセルが利用できなくなったか、またはそれ以前の任意のタイミングで、ICカード200から出力したログセットをまとめて履歴管理センタ130に送付する。このときユーザはICカード200から出力したログセットをログセットシリアル番号順に送信することが望ましいが、履歴管理センタ130でログセットシリアル番号をソーティングできればその必要はない。但し、出力したログセットが全て揃っている必要がある。図12は、履歴管理センタにおけるログセットの検証手順を示すフローチャートである。この処理は全て、履歴管理センタ130のコンピュータで行われる。

〔S31〕ログセットを受け取る。

〔S32〕受け取った複数のログセットをシリアル番号順にソートすると共に、ユーザIDを基にユーザDB900から対応するユーザの履歴管理用データ910を取得し、今回受け取ったシリアル番号の最小値が履歴管理センタ130で保管している、ユーザの前の最終ログセットシリアル番号912と連鎖していることを確認する。次に、今回受け取った複数のログセットのシリアル番号の連鎖を確認しログセットに抜けが無いことを確認したらステップS33に進む。ログセットに抜けがあった場合はステップS35に進む。

〔S33〕ログセットの署名に格納されている検証値7

05を用いてログの連鎖の検証を行う。検証が正しく行われればステップS34に進み、検証値が正しく行われなければステップS35に進む。なお、検証手順の詳細は後述する。

【S34】利用延長データを発行し、PC110へ転送する。

【S35】PC110にエラーステータスを返す。

【0057】これにより、ユーザは利用延長データを取得することが出来る。図13は、検証値の検証手順の詳細を示す図である。この処理は、全て履歴管理センタ130のコンピュータで行われる。

【S331】ログセットの検証を行う。検証には、ログセット500中の複数のログ512a～512n等を用いる。ここで、ログセットが複数ある場合には、シリアル番号順に検証が行われる。

【0058】まず、ログセットの出所が正しいことを検証する。これは、ログセット500内の署名値504をユーザID501に対応したICカード200の公開鍵により検証し、ログセット500の値と署名値の平文700中のデータとの整合を確認する。

【0059】次に最初のログ512aと前回の検証値913とを連結し、ICカード200が検証値を生成するのと同じ方法で、検証値を生成する。すなわち、結合された値に対して方向性ハッシュ関数MD5を用いてメッセージ・ダイジェストを計算し、検証値913aを生成する。

【0060】次にログ512bと検証値913aとを連結し、検証値913bを生成する。以下ログ512c～ログ913nまで、同様の演算を繰り返し、ログ512nと検証値913mの結合値に対するメッセージ・ダイジェストである検証値913nを生成する。

【S332】検証値705と検証値913nとを比較し、値が一致する場合にはステップS333に進む。検証値705と検証値913nとが一致しない場合はステップS334に進む。

【S333】次のログセットが存在する場合は上記と同様の手順で検証値を検証し、次のログセットが存在しない場合、すなわちユーザから受け取ったログセットの検証が全て終了した場合は、履歴管理センタで管理しているユーザの履歴管理データ910中の前回の最終シリアル番号912を今回検証した最後のログセットのシリアル番号で更新し、前回の最終検証値913を今回検証した最後のログセットの検証値で更新する。

【S334】エラーステータスをユーザに返し、処理を終了する。

【0061】このようにして、履歴管理センタ130がログセットを検証し、利用延長データを発行する。図14は、利用延長データの構成例を示す図である。この図は、利用延長データの署名前の平文800を示している。この平文800には、生成可能ログ数801、有効

期限802、検証値803を含んでいる。ここでの検証値803には最後に検証したログセットの検証値が入る。履歴管理センタ130ではこの平文800に対して履歴管理センタ130の秘密鍵で署名し、利用延長データとしてユーザに送信する。

【0062】ユーザは、受け取った利用延長データをICカード200に入力する。ICカード200では、利用延長データ認証部208が利用延長データの署名を予め登録されている履歴管理センタ130の公開鍵で検証する。さらに、利用延長データ中の検証値803と検証値格納部202内の検証値が一致したら、ICカード200の利用期限207aを利用延長データ中の有効期限802で更新し、生成可能ログ数減算カウンタ207bを利用延長データ中の生成可能ログ数801で更新する。また、ICカード200が停止状態の場合は、稼動制御部207が停止状態を解除する。

【0063】このように、本発明によれば利用履歴等の長大なデータをブロック化して、ユーザの任意のタイミングにおいてネットワークで安全に送付可能である。また、ブロック化されたデータごとに認証が可能であり、かつブロックの連鎖も認証することができる。また、本発明によればログデータがICカード等の履歴格納媒体の記憶容量を越える場合でも、一旦履歴格納媒体から履歴データを出力して、新たに格納することが可能なので、履歴データの管理を履歴格納媒体の記憶容量に何ら制限されずに行うことができる。

【0064】なお、以上の説明ではログセットが回収可能な場合の例を説明したが、何らかの事後によりログセットの一部が破壊された場合でも、本発明ではログセットをログシリアル番号で管理し、またログセットごとにICカードの署名を施しているため、破壊されたログセット以外の検証を行うことが可能である。

【0065】次に、第2の実施の形態について説明する。この実施の形態は、ログセットを出力してから利用延長データを受け取るまでの間にも、カプセル300を利用できるようにしたものである。すなわち、第1の実施の形態では、ログセット500を履歴管理センタ130に送付し利用延長データを受け取るまでに、カプセルを実行してしまうと、ICカード200内でログが新たに生成され検証値が更新されてしまう。すると、利用延長データを検証できない。この問題を防ぐために、ユーザが履歴管理センタ130にログセットを送付後、利用延長データを受け取るまでカプセルを利用できないようにすることが考えられるが、ネットワークを利用するとしても、ある程度の時間ユーザはカプセル300を使用できなくなり不便である。そこで第2の実施の形態では、ユーザが履歴管理センタ130にログセットを送付後でも、ICカード内にログを保管できる範囲内であればカプセルを利用可能としている。

【0066】なお、本実施の形態は、第1の実施の形態

と比べ利用延長データ認証部208の処理機能が異なるだけであるため、第1の実施の形態の各要素に付加した符号を用いて本実施の形態を説明する。

【0067】図15は、第2の実施の形態における利用延長データの認証処理を示す図である。ここでは、ユーザが履歴管理センタ130に対しこれまでに出力したログセットを送付した後、カプセルをn回利用した場合を想定する。図に示すように、ログセット格納部204にはn個のログ204a~204nが格納されている。この状態で、ユーザが履歴管理センタ130から利用延長データ800を受け取り、ICカード200へ入力すると、以下の処理が行われる。

【S41】ICカード200では、利用延長データ認証部208が、利用延長データの署名を履歴管理センタ130の公開鍵で検証し利用延長データ中の検証値803を取得する。つぎに、ログセット格納部204内の最初のログ204aと利用延長データ中の検証値803を連結して、MD5演算部203が検証値を生成するときと同じ方法で検証値803aを生成する。以下同様にログ204b~204nと生成された検証値803a~803mにより、順次検証値が生成され最後に検証値803nが生成される。

【S42】利用延長データ認証部208が、検証値格納部202内の検証値202aと検証値803nとを比較し、それぞれの値が一致した場合はステップS43に進み、一致しなかった場合はステップS44に進む。

【S43】利用延長データ認証部208が、ICカード200の利用期限207aを利用延長データ中の有効期限802で更新し、生成可能ログ数減算カウンタ207bを利用延長データ中の生成可能ログ数801からログ数カウンタ204aの値(=n)を減算した値で更新する。さらに、ICカード200が停止状態の場合は、稼働制御部207が停止状態の解除を行う。

【S44】検証値202aと検証値803nとが一致しなかった場合は、利用延長データ認証部208が処理を中断しエラーを返す。

【0068】このようにして、ログセットを出力してから利用延長データを受け取るまでの間においても、カプセルを使用することが可能となる。なお、以上の例ではICカード内で、ログセットに格納されたログの検証値を検証することで利用延長データ中の検証値を検証したが、別の方法としては、検証値格納部202に格納される検証値とは別に、第2の検証値として前回出力されたログセットの検証値を保管しておき、利用期限データ中の検証値と第2の検証値とを比較して利用延長データ中の検証値を検証を行うことも考えられる。

【0069】なお、上記のICカードの有する機能の処理内容は、ROMに格納されたプログラムをICカード内のCPUが実行することで実現されているが、このプログラムを他のコンピュータで読み取り可能な記録媒体

に格納しておくこともできる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場を流通させる場合には、CD-ROMやフロッピーディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

【0070】

【発明の効果】以上説明したように本発明の被検証データ生成装置では、データ生成手段がデータ本文を生成する度に、そのデータ本文を用いて検証値を生成し、その検証値を用いて被検証データの署名値を生成するようにしたため、署名付きの被検証データを端末装置などに保管しておき、ユーザの任意のタイミングにおいてネットワークで安全にセンタに送付できる。また、被検証データごとに認証が可能であり、かつ被検証データの連鎖も認証することができるため、データ格納手段に長大なデータを保存する必要がなくなり、データ格納手段の記憶容量が少なくてすむ。

【0071】また、本発明のデータ検証装置では、データの検証を行う度に、最後に得られた検証値を保持しておき、保持している検証値を用いて次の被検証データの検証を行うようにしたため、被検証データの連鎖を認証することができる。

【0072】また、本発明の被検証データ生成プログラムを記録した媒体では、記録されているプログラムをコンピュータに実行させれば、データ生成手段がデータ本文を生成する度にそのデータ本文を用いた検証値を生成し、その検証値を用いて署名値を生成するような機能をコンピュータに持たせることができるため、端末装置などに一時的に保管しても不正を働くことが出来ないような連鎖性を保証した被検証データをコンピュータに生成させることが可能となる。

【図面の簡単な説明】

【図1】本発明の原理構成図である。

【図2】ICカードを用いた履歴管理システムの概略構成を示す図である。

【図3】カプセル化されたソフトウェアの構成を示す図である。

【図4】ICカードのハードウェア構成を示す図である。

【図5】ICカードの処理機能を示すブロック図である。

【図6】カプセル実行開始手順を示すフローチャートである。

【図7】ログの構成例を示す図である。

【図8】署名付きログセットの構成を示す図である。

【図9】ログセットの署名値として署名される平文の構成例を示す図である。

【図10】ICカードからログセットを出力する手順を示すフローチャートである。

【図11】履歴管理センタで管理しているユーザDBの例を示す図である。

【図12】履歴管理センタにおけるログセットの検証手順を示すフローチャートである。

【図13】検証値の検証手順の詳細を示す図である。

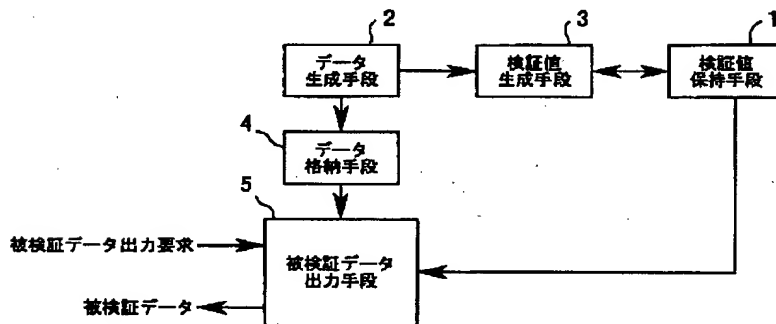
【図14】利用延長データの構成例を示す図である。

【図15】第2の実施の形態における利用延長データの認証処理を示す図である。

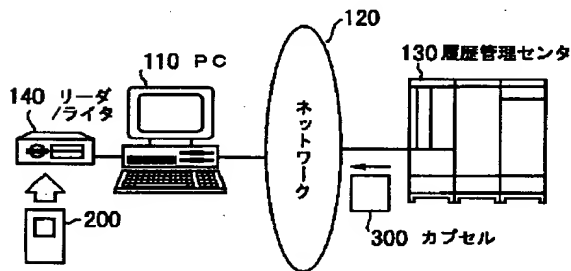
【符号の説明】

- 1 検証値保持手段
- 2 データ生成手段
- 3 検証値生成手段
- 4 データ格納手段
- 5 被検証データ出力手段

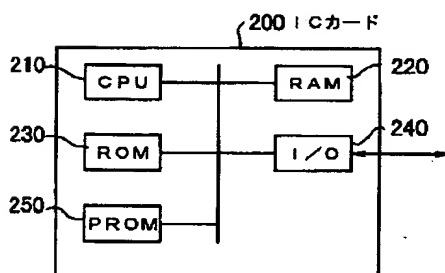
【図1】



【図2】



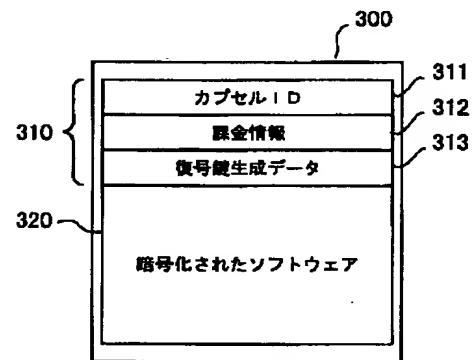
【図4】



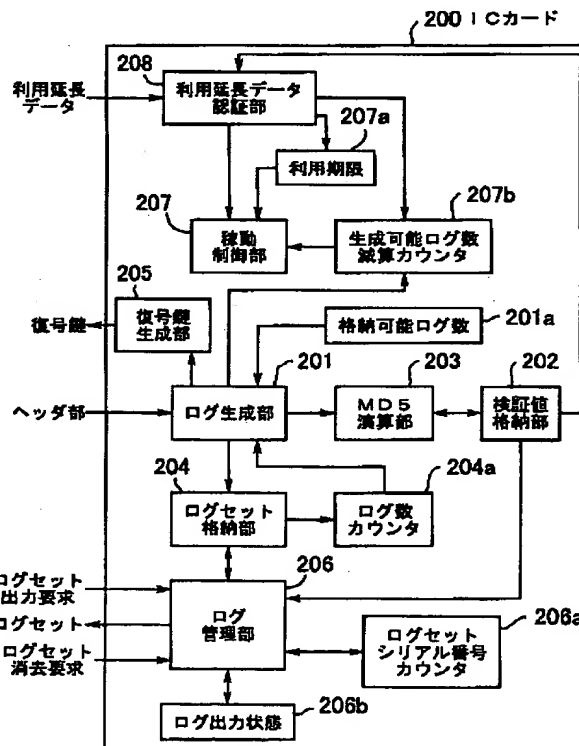
【図7】



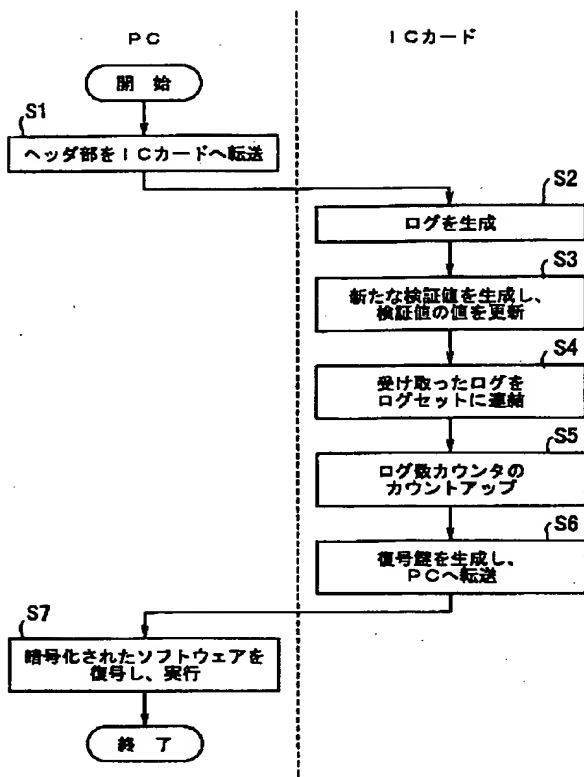
【図3】



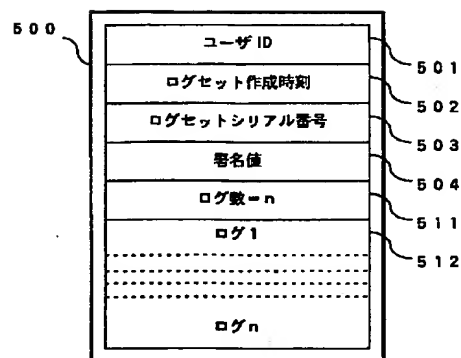
【図5】



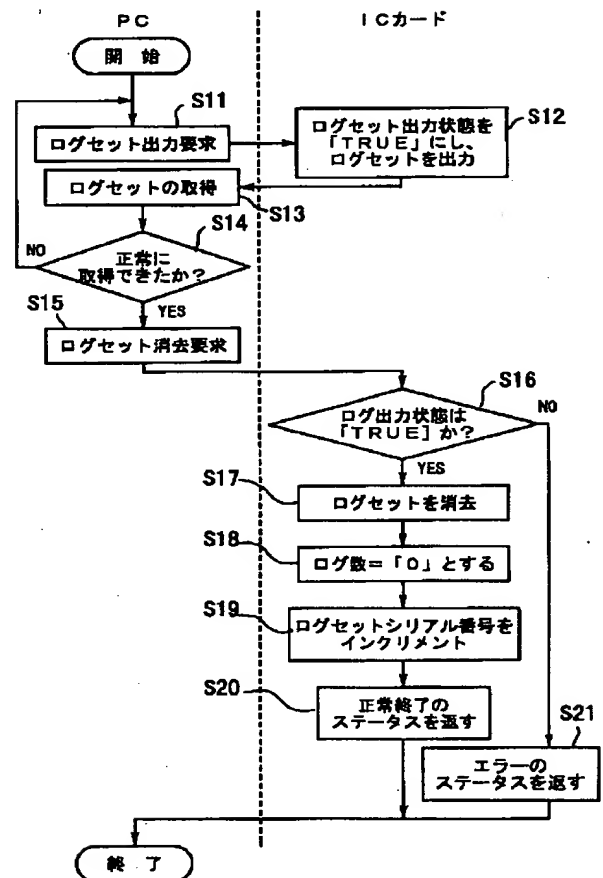
【図 6】



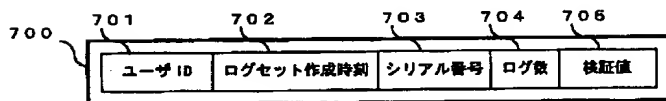
【図 8】



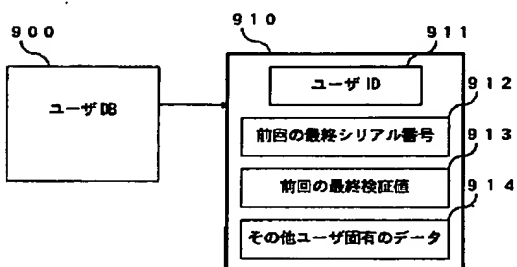
【図 10】



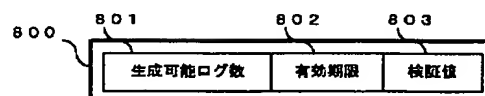
【図 9】



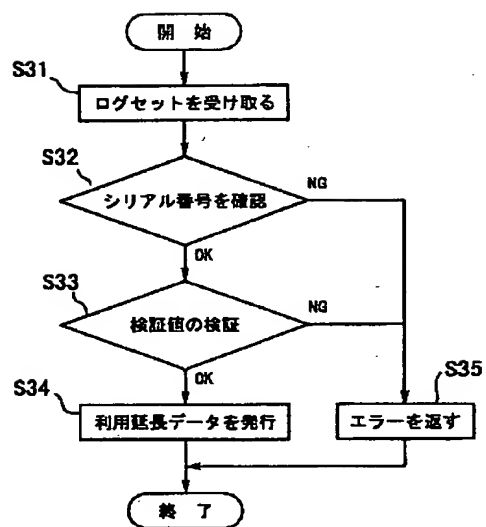
【図 11】



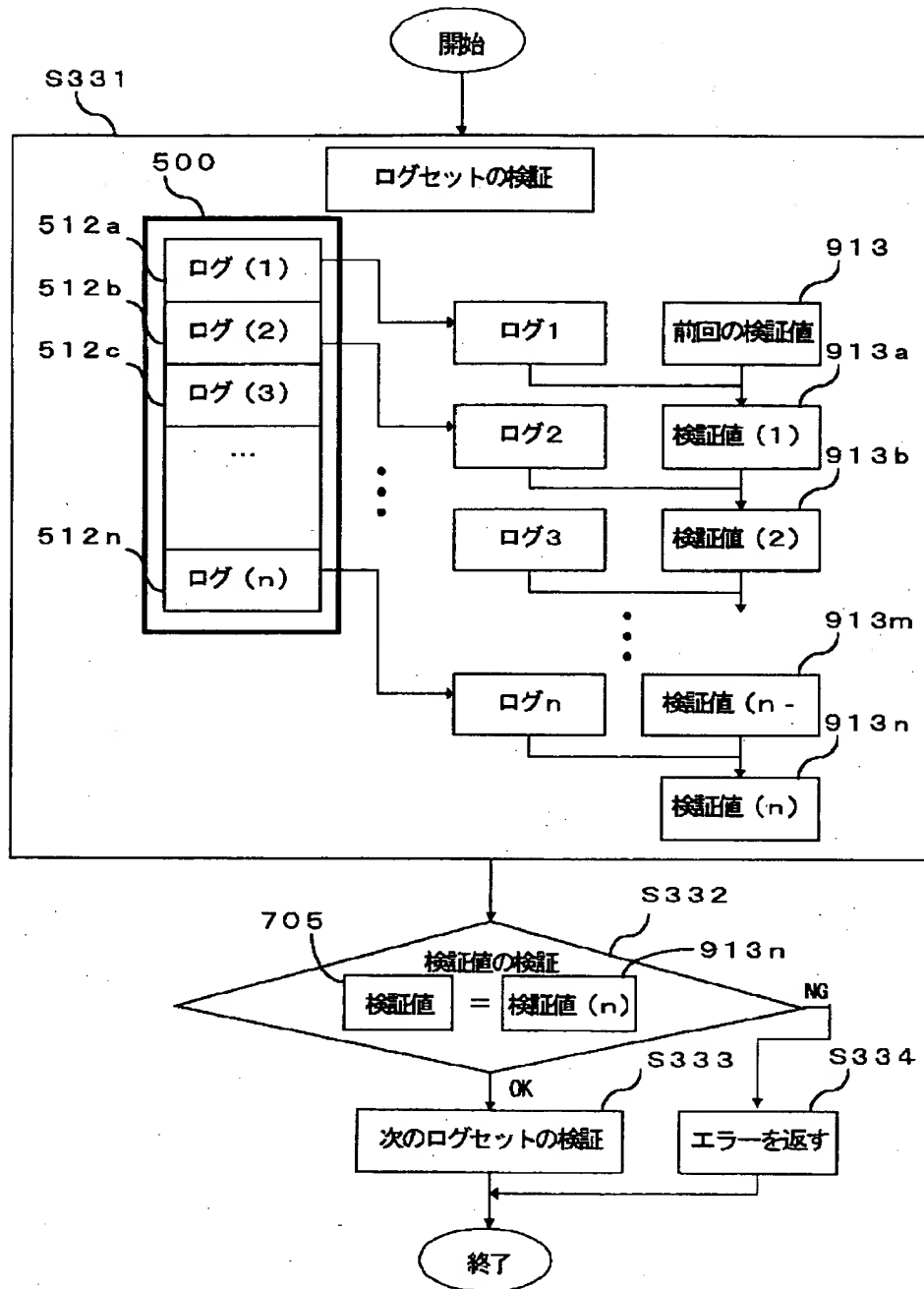
【図 14】



【図12】



【図13】





【図15】

